V. REMARKS

A. Status of the Claims

The Office Action has been received and carefully considered. Claims 1-2, 5-8 and 12-22 are currently pending. Claims 3, 4, 9, 10 and 11 have been previously cancelled. Claims 1 and 15 have been amended. No new matter is introduced by these amendments, and these amendments are fully supported by the specification. Applicant respectfully requests reconsideration of the rejections of the pending claims for at least the following reasons.

B. Objection To The Abstract

The Abstract has been objected to because it exceeds 150 words. Applicant has amended the Abstract accordingly.

C. Use Of Trademarks

The Specification stands objected to because it allegedly for using trademarks. In particular, the Office Action states:

> In paragraph 10 line 4, MICROSOFT WINDOWS is used. In paragraph 12 lines 5, 8 and 9, WAYPORT is used. In paragraph 13 lines 1, 2, 4, 6, 9, 10 and 13, BOINGO is used. In paragraph 41 line 4, CRYPTOFLEX is used

Office Action, Page 2. Applicant have amended paragraphs 10, 12, 13 and 41 appropriately.

D. Amendments To The Specification

The Office Action has requested that the "Cross-Reference To Related Applications" be updated. Accordingly, Applicant has submitted an amended paragraph 1 that includes the now-known related application numbers and corrected a typographical error.

E. Objections To The Drawings

The Drawings stand objected to because reference character 550 in Fig. 5A is allegedly used to designate both "Copy BBSID, MKS, and MKR to client Key" and "Exit." Office Action, Page 3. Applicant has submitted a replacement Fig. 5A.

F. Claim Rejections Under 35 U.S.C. § 112, ¶ 2

Claim 17 stands rejected under 35 U.S.C. § 112, ¶ 2, a allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Office Action asserts that "it is not clear which of the IEEE 802.11 family protocols/standards" claim 17 refers. Applicant respectfully disagrees.

IEEE 802.11 is a set of standards for implementing wireless local area network. The standards embraced by IEEE 802.11 are recognized and understood by those of skill in the art. According to the MPEP, "[i]f the scope of the subject matter embraced by the claims is clear, and if applicants have not otherwise indicated that they intend the invention to be of a scope different from that defined in the claims, then the claims comply with 35 U.S.C. 112, second paragraph." MPEP 2173.04. Therefore, Applicant respectfully requests that this rejection be withdrawn.

G. Claim Rejections under 35 U.S.C. § 103(a)

1. Claims 1-2 and 15-17

Claims 1-2 and 15-17 stand rejected under 35 U.S.C. 103(a) as allegedly rendered obvious by U.S. Patent Application Publication No. 2004/0198220 to Whelan *et al.* ("Whelan") in view of Menezes *et al.*, "Handbook of Applied Cryptography," 5th ed., June 2001, CRC Press ("Menezes"). Specifically, the Office Action admits that Whelan does not disclose an authentication process comprising the steps of:

> transmitting, by the client to the computing device, a first challenge, wherein said first challenge comprises an encrypted first random number and a unique identifier associated with said computing device, said encrypted first random number being encrypted with said first cryptographic key.
>
> receiving, by the client from the computing device, a second challenge, wherein said second challenge comprises an encrypted second random number, said second random number generated at said computing device and encrypted with a second cryptographic key, said second cryptographic key being obtained by said computing device and associated with said computing device identifier.

Office Action, Page 6. Thus, the Office Action refers to Menezes, which allegedly discloses:

> in protocol 12.39 on page 508 a modified Needham-Schroeder public key protocol wherein the client (A) sends B (the device) a challenge with rl and kl and the challenge is encrypted with PB. Similarly for the challenge between the device and the client.

Id. Thus, the Office Action contends that

> It would have been obvious to one of the ordinary skill in the art at the time of the Applicant's invention was made to modify the authentication process method of Whelan by a modified Needham-Schroeder public key protocol. The motivation/suggestion would have been to provide a mutual authentication between the client and the device communicating on a network.

Id.[1] Applicant respectfully disagrees as the Office Action has failed to establish a *prima facie* case of obviousness.

In order to establish a *prima facie* case of obviousness, at least three criteria must be met. First, there must be some motivation or suggestion to make the proposed combination or modification of the references. Second, there must be a reasonable expectation of success. Finally, the combined or modified references must teach or suggest all claim limitations. *See* MPEP 2142 *et seq.*

Independent claim 1 recites:

> 1. A method of authenticating a client to one or more computing devices at an edge of one or more communications networks, the method comprising the steps of:
>
> obtaining, by the client, a computing device identifier associated with a computing device;
>
> selecting, at said client, a set of authentication parameters associated with said computing device identifier, said authentication parameters being stored in a tamper-resistant physical token operatively coupled to said client, said tamper-resistant physical token further permanently storing a unique identifier associated with said client, said tamper resistant physical token further storing a first cryptographic key; and
>
> implementing an authentication process employing said set of authentication parameters, the authentication process comprising the steps of:
>
> transmitting, by the client to the computing device, a first challenge, wherein said first challenge comprises an encrypted first random number and said unique identifier associated with said client, said first random number being generated inside said tamper-resistant physical token, said encrypted first random number being encrypted with said first cryptographic key;
>
> receiving, by the client from the computing device, a second challenge, wherein said second challenge comprises an encrypted second random number, said second random number generated at said computing device and encrypted with a second cryptographic key, said second cryptographic key being obtained by said computing device and associated with said computing device identifier; and

[1] Notably, the Office Action no longer bases this rejection on the inclusion of U.S. Patent Publication No. 2001/0023446 to Balogh.

> permitting, at said client, said client to access said communications network via said computing device if said authentication process results in a successful authentication of said client.

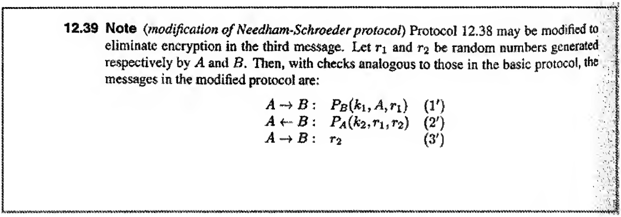
Appl'n, Claim 1 (emphasis added). First, and without conceding that the proposed combination of Whelan and Menezes is proper, Applicant s note that Whelan does not disclose "said authentication parameters being stored in a tamper-resistant physical token operatively coupled to said client, said tamper-resistant physical token further permanently storing a unique identifier associated with said client, said tamper resistant physical token further storing a first cryptographic key." Indeed, the Office Action previously admitted that Whelan does not disclose this element. *See* Office Action mailed January 30, 2007 at 6 ("Whelan ... did not disclose set of authentication parameters are prestored in a tamper-resistant physical token."). The paragraph cited by the Office Action in support of this allegation does not disclose or suggest the use of a tamper resistant physical token. *See* Office Action, Page 5 (citing Whelan, ¶ 43). For convenience, paragraph 43 of Whelan is reproduced below:

> [0043] When mobile units 28 roam to new sub-networks 18 or are initialized, one or more security servers 10 authenticate the mobile units 28, typically using security information stored by the server 14 and in the mobile unit 30. The security server also provides a means for the mobile units to authenticate associations with access points 20, typically using Simple Network Management Protocol (SNMP) traps 22 and MU association lists 36.

Whelan, ¶ 43. As the Office Action mailed January 30, 2007 correctly recognized, Whelan does not disclose that authentication parameters are stored in a tamper-resistant physical token. As Menezes also fails to disclose this element, Applicant respectfully requests that this rejection be withdrawn.

Further, Applicant has amended claims 1 and 15 to specify that the authentication is "at an edge of one or more communications networks." Applicant has defined "edge" to refer to "authentication of client devices taking place at the edge or outer boundary of the network, i.e., at the access point, rather than centralized within the network using a server." Appl'n, ¶ 40. Whelan, however, does not disclose authentication at an edge of a communication network. Instead, Whelan discloses that security server 10 (*see* Fig. 1) performs the authentication. *See* Whelan, ¶ 43 ("When mobile units 28 roam to new sub-networks 18 or are initialized, one or more security servers 10 authenticate the mobile units 28, typically using security information stored by the server 14 and in the mobile unit 30."). Whelan's security server is not on the edge of a communication network, and Menezes does not disclose authentication at the edge of the communication network. Therefore, because the proposed combination of Whelan and Menezes fail to disclose this element, Applicant respectfully requests that this rejection be withdrawn.

In addition. the proposed combination fails to disclose the claimed authentication process because Menezes' "modified Needham-Schroeder public key protocol" is not the same as the claimed authentication protocol. For convenience, the relevant section of Menzes is reproduced below:



12.39 Note *(modification of Needham-Schroeder protocol)* Protocol 12.38 may be modified to eliminate encryption in the third message. Let r_1 and r_2 be random numbers generated respectively by A and B. Then, with checks analogous to those in the basic protocol, the messages in the modified protocol are:

$$\begin{array}{lll} A \rightarrow B: & P_B(k_1, A, r_1) & (1') \\ A \leftarrow B: & P_A(k_2, r_1, r_2) & (2') \\ A \rightarrow B: & r_2 & (3') \end{array}$$

The Office Action asserts that, applying this protocol to Whelan, the client is "A," while the device is "B." Thus, in step 1', the client sends the device the device's public-key encryption of the concatenation of session key 1 (k_1), A, and a random number 1 (r_1) generated by the client. In step 2', the device sends to the client the client's public-key encryption of the concatenation of session key 2 (k_2), random number 1 (r_1), and random number 2 (r_2) generated by the device. Finally, in step 3', the client sends to the device unencrypted random number 2.

With this understanding, it is clear that this protocol is not the same as the claimed authentication process. First, in the claimed authentication protocol, neither the client's nor the device's session keys are transmitted or received. Instead, as claimed, the first challenge includes an encrypted first random number and the unique identifier that is associated with the client. The second challenge includes an encrypted second random number.

Second, the claims expressly require that the computing device uses a "second cryptographic key" that is "associated with said computing device identifier." Clearly, under the modified Needham-Schroeder public key protocol, the message that is sent from the device (B) to the client (A) is encrypted with the client's public session key.

Third, the modified Needham-Schroeder public key protocol requires three separate transmissions in order to complete the authentication. The present authentication is a two-step authentication.

For at least these reasons, the proposed combination of Whelan and Menezes fails to disclose or suggest all claim elements of independent claims 1 and 15, and Applicant respectfully requests that the rejection of these claims and all claims dependent thereon be withdrawn.

2. Claims 5-8, 12, and 18-22

Claims 5-8, 12, and 18-22 stand rejected under 35 U.S.C. § 103(a) as allegedly rendered obvious by Whelan and Menezes in further in view of U.S. Patent Application Publication No. 2001/0023446 to Balogh.[2] Applicant notes that claims 5-8 and 12 are dependent on independent claim 1, and claims 18-22 are dependent on independent claim 15, which are allowable for at least the reasons set forth above. Balogh fails to cure the deficiencies with the proposed combination of Whelan and Menezes. Thus, these claims are also nonobvious. *See* MPEP § 2143.03 ("If an independent claim is nonobvious under 35 U.S.C 103, then any claim depending therefrom is nonobvious.") (quoting *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988)). Therefore, Applicant respectfully request that the rejections of these claims be withdrawn.

3. Claims 13 and 14

Claims 13 and 14 stand rejected under 35 U.S.C. § 103(a) as allegedly rendered obvious by Whelan and Menezes in further in view of U.S. Patent No. 5,661,806 to Nevoux *et al.* Applicant notes that 13 and 14 are dependent on independent claim 1, which is allowable for at least the reasons set forth above. Balogh fails to cure the deficiencies with the proposed combination of Whelan and Menezes. Thus, these claims are also nonobvious. *See* MPEP § 2143.03 ("If an independent claim is nonobvious under 35 U.S.C 103, then any claim depending

[2] Applicant note that, in its rejection, the Office Action asserts that "Balogh discloses installing the tamper-resistant physical token at the computing device." Office Action, Page 7. Applicant notes, however, that the claim recites "installing said tamper-resistant physical token at said client," not at the computing device.

therefrom is nonobvious.") (quoting *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988)). Therefore, Applicant respectfully request that the rejections of these claims be withdrawn.

VI. CONCLUSION

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance, and an indication of the same is courteously solicited. The Examiner is cordially invited to contact the undersigned by telephone at the below-listed telephone number, in order to expedite resolution of any outstanding issues. Applicant believes that no fees are necessary to maintain the instant application pending. However, should the Commissioner determine that any fees are necessary, the U.S. Patent and Trademark Office is authorized to charge such fees to the undersigned's Deposit Account No. 50-0206.

Respectfully submitted,
HUNTON & WILLIAMS LLP

Dated: April 13, 2009 By: ______________________
Robert A. King
Registration No. 42,738

Hunton & Williams LLP
Intellectual Property Department
1900 K Street, N.W., Suite 1200
Washington, DC 20006
(404) 888-4060 (Telephone)
(404) 888-4190 (Facsimile)